Attorney's Docket No. 032326-293

10/523840

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BT01 Rec'd PCT/PTO 08 FEB 2005

In re Patent Application of	
Olivier Billet et al.	Group Art Unit:
Application No.: Unassigned	Examiner:
Filed: February 8, 2005	Confirmation No.:
For: UNIVERSAL CALCULATION METHOD APPLIED TO POINTS ON AN ELLIPTIC CURVE DEFINED BY A QUARTIC, AND ASSOCIATED CRYPTOGRAPHIC METHOD AND ELECTRONIC COMPONENT	

FIRST INFORMATION DISCLOSURE STATEMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the duty of disclosure as set forth in 37 C.F.R. § 1.56, the accompanying information is being submitted in accordance with 37 C.F.R. §§ 1.97 and 1.98.

The listed documents are cited in the International Search Report in the corresponding PCT application.

To assist the Examiner, the documents are listed on the attached form PTO-1449. However, copies of the documents are not provided as it is understood that they have already been transmitted by the International Bureau. It is respectfully requested that an Examiner initialed copy of this form be returned to the undersigned.

Respectfully submitted,

BURNS, DOANE, SWECKER & MATHIS, L.L.P.

Date February 8, 2005

By: _____
James A. LaBarre
Registration No. 28,632

P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620

(8/04)

Substitute for form 1449A/PTO & 1449B/PTO

FIRST INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet 1 of 1

Complete if Known	
Application Number	10/523840
Filing Date	February 8, 2005
First Named Inventor	Olivier Billet et al.
Examiner Name	
Attorney Docket Number	032326-293

U.S. PATENT DOCUMENTS

Examiner Initials	Document Number	Kind Code (if known)	Name of Patentee or Applicant of Cited Document	Issue/Publication Date (MM-DD-YYYY)

FOREIGN PATENT DOCUMENTS

Examiner Initials	Document Number	Kind Code (if known)	Country	Date of Publication (MM-DD-YYYY)	STATUS: Translation	Partial Translation	Eng. Lang. Summary	Search Report	IPER	Abstract	Cited in Spec

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.
	CHUDNOVSKY D.V. et al., "Sequences of Numbers Generated By Addition In Formal Groups and New Primality and Factorization Tests", Advances in Applied Mathematics, Academic Press, Vol. 7, 1986, pages 385-434.
	BRIER E. et al., "Weierstrass Elliptic Curves and Side-Channel Attacks", 5th International Workshop on Practice and Theory in Public Key Cryptosystems, February 2002, pages 335-345.
	JOYE M. et al., "Hessian Elliptic Curves and Side-Channel Attacks", Cryptographic Hardware and Embedded Systems Ches, Third International Workshop, Vol. 2162, May 14, 2001, pages 402-410.
	KHELDOUNI A. et al., "Elliptic Cohomology Operation Defined By Hecke Operator T2", Vol. 324, No. 2, January 1997, pages 215-220.
	P. BARRETO et al., "Constructing Elliptic Curves With Prescribed Embedding Degrees", Security in Communication Networks, Third International Conference, September 2002, pages 257-267.

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with M.P.E.P. § 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to Applicant.